WHAT IS CLAIMED IS:

1. A method for protecting an electronic document, comprising:

encrypting the electronic document using a document encryption key;

generating a multi-key encryption table for use in a multi-key encryption method, the table comprising at least one multi-key component;

generating an encrypted header comprising information pertaining to the electronic document;

associating a user interface device with the encrypted header , the multi-key encryption table and the encrypted electronic document, wherein the user interface device comprises unencrypted information for identifying the electronic document and an interactive element for enabling a user to input a user authorization for access to at least a portion of the encrypted electronic document;

combining the user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the encrypted header; and

upon a valid decryption of the encrypted header, decrypting the portion of the encrypted electronic document.

2. The method of claim 1, wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates that the document encryption key has been found.

3. The method of claim 1, wherein the electronic document comprises content information that is formatted based on an object language having a set of formatting rules.

4. The method of claim 3, wherein the user interface device comprises a second electronic document.

5. The method of claim 1, wherein the information pertaining to the electronic document comprises a user permission table for access to all or portions of the electronic document and wherein only those permitted portions of the electronic document are decrypted.

6. The method of claim 1, wherein the encrypted header and the encrypted electronic document are encrypted using different encryption keys and wherein the multi-key encryption table includes at least one multi-key component for each encryption key.

7. The method of claim 1, wherein the encrypted header further comprises a fingerprint for identifying some predefined aspect of the electronic document.

8. The method of claim 1, wherein the electronic document comprises a plurality of individual electronic documents and the encrypted header comprises information pertaining to each of the individual electronic documents.

9. The method of claim 8, wherein the information pertaining to the electronic document comprises a user permission table setting forth access to all or portions of each of the individual electronic documents and wherein only those permitted portions of the authorized electronic document are decrypted.

10. The method of claim 3, wherein the content information is selected from the group consisting of text, graphics, equations, tables, spreadsheets, pictures, video files, audio files, multimedia files and binary data of unknown format.

11. The method of claim 1, wherein the object language comprises Adobe Acrobat.

12. The method of claim 1, wherein the object language comprises a language which interprets Microsoft Word documents.

13. The method of claim 6, wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the header encryption key has been found; and wherein the encrypted electronic document includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the document encryption key has been found.

14. The method of claim 1, wherein the electronic document includes a document ID and wherein the document encryption key includes a combination of the document ID, the user information and the multi-key component, for each authorized user.

15. A secure content object, comprising:

an encrypted electronic document having been encrypted with a document encryption key;

an encrypted header comprising information pertaining to the electronic document;

a multi-key encryption table for use in a multi-key encryption method, the table comprising at least one multi-key component;

a user interface device comprising unencrypted information for identifying the electronic document and an interactive element for enabling a user to input a user authorization for access to at least a portion of the encrypted electronic document, for inputting the user authorization to a decryption engine using the multi-key encryption method for combining the user authorization with each of the multi-key components in the multi-key encryption key table to decrypt the encrypted header, and

upon a valid decryption of the encrypted header, for enabling decryption of the portion of the encrypted electronic document.

16. The secure content object of claim 15, wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable

variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the document encryption key has been found.

17. The secure content object of claim 15, wherein the electronic document comprises content information that is formatted based on an object language having a set of formatting rules.

18. The secure content object of claim 15, wherein the user interface device comprises a second electronic document.

19. The secure content object of claim 15, wherein the information pertaining to the electronic document comprises a user permission table for access to all or portions of the electronic document and wherein only those permitted portions of the electronic document are decrypted.

20. The secure content object of claim 15, wherein the encrypted header and the encrypted electronic document are encrypted using different encryption keys and wherein the multi-key encryption table includes at least one multi-key component for each encryption key.

21. The secure content object of claim 15, wherein the encrypted header further comprises a fingerprint for identifying a predefined aspect of the electronic document.

22. The secure content object of claim 15, wherein the electronic document comprises a plurality of individual electronic documents, the encrypted header comprises information pertaining to each of the individual electronic documents.

23. The secure content object of claim 22, wherein the information pertaining to the electronic document comprises a user permission table setting forth access to all or

portions of each of the individual electronic documents and wherein only those permitted portions of the authorized electronic document are decrypted.

24. The secure content object of claim 17, wherein the content information is selected from the group consisting of text, graphics, equations, tables, spreadsheets, pictures, video files, audio files, multimedia files and binary data of unknown format.

25. The secure content object of claim 15, wherein the object language comprises Adobe Acrobat.

26. The secure content object of claim 15, wherein the object language comprises a language which interprets Microsoft Word documents.

27. The secure content object of claim 20, wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the header encryption key has been found; and wherein the encrypted electronic document includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the document encryption key has been found.

28. The secure content object of claim 15, wherein the electronic document includes a document ID and wherein the document encryption key includes a combination of the document ID, the user information and the multi-key component, for each authorized user.

29. The secure content object of claim 15, wherein the electronic document comprises a first electronic document and an annotation associated therewith, wherein the annotation is encrypted using an encryption key associated with a user generating the

annotation; and wherein the encrypted header includes information pertaining to the first electronic document and the annotation.

30. The secure content object of claim 1, wherein the multi-key encryption table is located remote from the user interface device.

31. A system for protecting an electronic document, comprising:

a memory storing a secure content object and a multi-key encryption key table for use in a multi-key encryption method, the table comprising at least one multi-key component;

wherein the secure content object comprises an encrypted electronic document having been encrypted with a document encryption key and an encrypted header, wherein the encrypted header comprises information pertaining to the electronic document, and a user interface device comprising unencrypted information for identifying the electronic document and an interactive element for enabling a user to input a user authorization for access to at least a portion of the encrypted electronic document and, upon a valid decryption of the encrypted header, for enabling decryption of the portion of the encrypted electronic document;

a decryption engine which uses a multi-key encryption method; and

a processor for executing the interactive element and for inputting the user authorization to the decryption engine;

wherein the decryption engine combines the user authorization with each of the multi-key components in the multi-key table to decrypt the encrypted header, wherein a valid decryption of the encrypted header indicates the document encryption key has been found.

32. The system of claim 31, wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the document encryption key has been found.

33. The system of claim 31, wherein the electronic document includes a document ID and the document encryption key includes a combination of the document ID, the user information and the multi-key component, for each authorized user.

34. A method for creating a document with secure annotations, comprising:

providing an electronic document;

providing an annotation pertaining to the electronic document;

encrypting the annotation using an encryption key associated with a user generating the annotation, wherein access to the encrypted annotation is available to users having access to the annotation encryption key;

associating the encrypted annotation with the electronic document such that access to electronic document is provided to at least one user and access to the encrypted annotation is provided only to users having the annotation encryption key.

35. A method for creating a document with secure annotations, comprising:

providing an electronic document, wherein access to the electronic document is available to a first set of users;

generating a plurality of annotations pertaining to the electronic document using the document language;

encrypting each annotation using an annotation encryption key associated with a user generating the particular annotation, wherein access to an encrypted annotation is available to users having access to the respective annotation encryption key;

concatenating the plurality of encrypted annotations in a second electronic document; and

associating the second electronic document with the electronic document such that access to the electronic document is available to the first set of users and access to the encrypted annotations in the separate file is provided only to users having the required encryption keys.

36. The method of claim 35, further comprising the step of merging the second electronic document and the electronic document into a third electronic document.

37. The method of claim 35, further comprising the step of encrypting the first electronic document using a document encryption key, wherein access to the encrypted electronic document is provided only to users having the required encryption key.

38. The method of claim 35, further comprising adding an unencrypted header identifying the generating user to each encrypted annotation.

39. The method of claim 35, further comprising, for each annotation encryption key:

generating a multi-key encryption table for use in a multi-key encryption method, the table comprising at least one multi-key component;

providing a user interface for enabling a user to input a user authorization for access to at least a portion of an encrypted annotation;

combining the user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the annotation, wherein valid decryption of the annotation indicates the correct annotation encryption key has been found.

40. The method of claim 39, further comprising, for each annotation encryption key:

generating a multi-key encryption table for use in a multi-key encryption method, the table comprising at least one multi-key component;

wherein each annotation includes an encrypted header;

providing a user interface for enabling a user to input a user authorization for access to at least a portion of the encrypted annotation;

combining the user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the encrypted header; and upon a valid decryption of the encrypted header, decrypting the portion of the encrypted annotation.

41. The method of claim 40, wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the annotation encryption key has been found.

42. The method of claim 35, wherein the separate file and the electronic document are stored in different locations.